РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АБСТРАКТНОГО АВТОМАТА

канд. техн. наук, проф. С.Ю. Гавриленко, студ. В.В. Челак,
Национальный технический университет "Харьковский политехнический институт", г. Харьков

Проблема быстродействия, точности и оптимизаций процессов выявления, и классификации вредоносного программного обеспечения в компьютерных системах является наиболее актуальной в области защиты информации, так как вирусы наносят экономический ущерб [1, 2].

В докладе представлена интеллектуальная система обнаружения и классифицирования вредоносного программного обеспечения на основе абстрактного автомата [3].

Работы системы заключается в анализе программного кода и подаче полученных выходных команд (групп команд) на вход абстрактного автомата. Каждая из команд сопоставляется с условием перехода из одного состояния S_i в другое S_{i+1} состояние с учетом значения маркера. Введение в абстрактную модель специальных коэффициентов "проходимости" или "маркеров", позволит уменьшить ложные срабатывания и увеличит спектр обнаружения модифицированных вирусов, Введение дополнительных переходов и зацикленность на состояниях также позволяют обнаружить модификацию известных вирусов, и приведет к оптимизации автомата по памяти, т.к. количество переходных состояний сокращается

Для идентификации состояния компьютерной системы была разработана программная модель обнаружения вирусов типа "червь" и их модификации с учетом наличия "маркеров".

Полученные результаты показали возможность использования интеллектуальной системы на основе абстрактного автомата как дополнительного средства для выявления вирусных атак в общей системе обнаружения вредоносного программного обеспечения.

Список литературы: 1. *Шелухин О.И.* Обнаружение вторжений в компьютерные сети / *О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова*. – М.: Горячая линия-Телеком, 2013. – 220 с. **2.** *Гошко С.В.* Технологии борьбы с компьютерными вирусами / *С.В. Гошко*. – М.: Солон-Пресс, 2009. – 352 с. **3.** *Гавриленко С.Ю.* Логіка дискретних автоматів / *С.Ю. Гавриленко, А.М. Клименко, В.І. Носков*. –Х: НТУ "ХПІ", 2014. – 129 с.